Security, Privacy, and Architecture of FieldAware Services

Last Updated: 10 January 2020

FieldAware's Corporate Trust Commitment

FieldAware is committed to achieving and maintaining the trust of our customers. Integral to this mission is providing a robust security and privacy program that carefully considers data protection matters across our suite of services, including data submitted by customers to our services.

Definitions

"Customer Data" means electronic data and content provided to FieldAware by Customer (or at its direction) via the Covered Services.

"Covered Services" means the FieldAware web, mobile, API, customer portal and connector services.

"Security Incident" means any unauthorized access to the Covered Services that results in unauthorized transmission, copy, disclosure, alteration or loss of Customer Data.

Services Covered

This documentation describes the architecture of, the security- and privacy-related audits and certifications received for, and the administrative, technical and physical controls applicable to the Covered Services.

Architecture and Data Segregation

The Covered Services are operated in a multitenant architecture that is designed to segregate and restrict Customer Data access based on business needs. The architecture provides an effective logical data separation for different customers via customer-specific "Organization IDs" and allows the use of customer and user role-based access privileges. Additional data segregation is ensured by providing separate environments for different functions, especially for testing and production.

Control of Processing

FieldAware has implemented procedures designed to ensure that Customer Data is processed only as instructed by the customer, throughout the entire chain of processing activities by FieldAware and its sub-processors. In particular, FieldAware have entered into written agreements with their sub-processors containing privacy, data protection and data security obligations that provide a level of protection appropriate to their processing activities. Compliance with such obligations as well as the technical and organizational data security measures implemented by FieldAware and its sub-processors are subject to audits. The "Infrastructure and Sub-processors" documentation describes the sub- processors.

Third-Party Functionality

Certain features of the Covered Services use functionality provided by third parties. The geocoding feature is provided by Google Maps. FieldAware only submits the name and address of locations for geocoding and not user or organisation names.

Audits and Certifications

The following security and privacy-related audits and certifications are applicable to the Covered Services:

- **CSA OWASP:** FieldAware follows OWASP Top 10 best practices and Cloud Security Alliance (CSA) Standards.
- **Service Organization Control (SOC) Compliance:** FieldAware is currently undergoing SOC 2 Type 1 and Type II compliance.

Security Controls

The Covered Services include a variety of configurable security controls that allow customers to tailor the security of the Covered Services for their own use.

Security Policies and Procedures

The Covered Services are operated in accordance with the following policies and procedures to enhance security:

- Customer passwords are stored using a one-way salted hash.
- User access log entries are maintained, containing date, time, user ID, URL executed or entity ID operated on, operation performed (created, updated, deleted) and source IP address. Note that source IP address might not be available if NAT (Network Address Translation) or PAT (Port Address Translation) is used by Customer or its ISP.
- Data centers used for the Covered Services maintain on-site security operations responsible for all physical data center security functions 24 hours a day, 7 days a week. These data centers are Tier 3 SOC 2 Type 2 certified computing facilities with controlled access.
- Data center physical access logs, system infrastructure logs, and application logs will be kept for a minimum of 90 days. Logs will be kept in a secure area to prevent tampering.
- Passwords are not logged
- FieldAware personnel will not set a defined password for a user. Passwords are reset to a random value (which must be changed on first use) and delivered automatically via email to the requesting user.

Security Logs

All systems used in the provision of the Covered Services, including firewalls, routers, network switches and operating systems, log information to their respective system log facility or a centralized syslog server (for network systems) in order to enable security reviews and analysis.

Incident Management

FieldAware maintains security incident management policies and procedures. FieldAware will notify impacted customers without undue delay of any unauthorized disclosure of their respective Customer Data of which FieldAware becomes aware to the extent permitted by law.

FieldAware typically notifies customers of significant system incidents by email, and for incidents lasting more than one hour, may invite impacted customers to join a conference call about the incident and FieldAware's response.

User Authentication

Access to Covered Services requires authentication via one of the supported mechanisms, which includes user ID/password, SAML based Federation or Token-Based Authentication (TBA) as determined and controlled by the customer. Following successful authentication, a random session ID is generated and stored in the user's browser to preserve and track session state.

Reliability and Backup

All networking components, network accelerators, load balancers, Web servers and application servers are configured in a redundant configuration. All Customer Data submitted to the Covered Services is stored on a primary database server with active database slaves for higher availability. All Customer Data submitted to the Covered Services is stored on highly redundant carrier-class disk storage and multiple data paths to ensure reliability and performance. All Customer Data submitted to the Covered Services, up to the last committed transaction, is automatically replicated on a near real-time basis to the secondary site and is backed up on a regular basis. Any backups are verified for integrity and stored in the same data centers as their instance.

Disaster Recovery

Production data centers are designed to mitigate the risk of single points of failure and provide a resilient environment to support service continuity and performance. The Covered Services utilize secondary facilities that are geographically diverse from their primary data centers, along with required hardware, software, and Internet connectivity, in the event FieldAware production facilities at the primary data centers were to be rendered unavailable.

Data Encryption

The Covered Services use industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and the Covered Services, including through Transport Layer Encryption (TLS) version 1.2. Additionally, all data, including Customer Data, is transmitted between data centers for replication purposes across a dedicated, encrypted link utilizing AES-256 encryption.

Return/Deletion of Customer Data

After termination of all subscriptions associated with an environment, Customer Data submitted to the Covered Services is retained in inactive status within the Covered Services for 90 days. During this 90-day period, if Customer has not downloaded their data prior to end of their subscription term, upon Customer's request FieldAware will grant customer limited access to the Service for several days for the sole purpose of permitting the Customer to retrieve their Customer Data, provided that the Customer has paid in full all good faith undisputed amounts owed to FieldAware. After this 90-day period the Customer Data is securely overwritten and deleted from production.

Interoperation with Other Services

The Covered Services may interoperate or integrate with other services provided by FieldAware or third parties. FieldAware also provides a variety of platforms and features that allow FieldAware users to learn about FieldAware products, participate in communities, connect third party applications, and participate in pilots, testing and assessments, which are outside the scope of this documentation.